WE CLAIM:

1. A device security method for verifying an authorized user, comprising:

storing an authorized user video image corresponding to authorized user identity data;

receiving a present user video image corresponding to user identity data;

determining image differences between the present user video image and the authorized user video image; and

in response to the determination of image differences and to a difference threshold level, determining whether to permit device usage.

2. The security method of claim 1, further comprising determining a quantity of the image differences between the present user video image and the authorized user video image, and disabling the device if the quantity of image differences exceeds the difference threshold level.

3. The security method of claim 1, wherein the authorized user video image is stored as first digital pixel data into a first memory, and wherein the present user video image is stored as second digital pixel data into a second memory, and wherein the quantity of image differences are determined quantitatively between the first and second digital pixel data.

4. The security method of claim 1, wherein the present user video image and the authorized user video image are each stored in MPEG4 format.

5. The security method of claim 1, wherein the authorized and present user video images are each framed to include only the head and face portions of the user.

6. The security method of claim 1, wherein the authorized and present user video images are scaled to the same proportions.

7. The security method of claim 1, wherein the device selected from the group of cellular telephone, videophone, video conferencing equipment, vehicle, and passageway.

8. The security method of claim 1, further comprising storing the present user video image in a present user video image log.

9. The security method of claim 1, further comprising transmitting the present user video image to a monitoring station if the differences exceed the difference threshold level.

10. The security method of claim 1, further comprising requesting alternate authorization if the differences exceed the difference threshold level.

11. The security method of claim 1, further comprising confirming motion within the present user video image before determining quantity of image differences.

12. A video security apparatus, comprising:

a video image input means for producing a user video image;

a user video image digitizing means for creating a digital representation of the user video image;

a user video reference image memory for storing at least one digital user video image as a user video reference image;

a user video reference image control means for controlling access to the user video reference image memory;

a comparison means for determining difference information between the user video reference image and the user video image;

an authentication means for determining an identity mismatch from the difference information; and

an output for communicating the identity mismatch.

13. The video security apparatus of claim 12, wherein the output communicates the identity mismatch by transmitting the user video image to a monitoring station

14. The video security apparatus of claim 12, wherein the output communicates the identity mismatch by disabling the image input means.

16. An interframe coding method for performing predictive coding using a stored authorized user video image corresponding to authorized user identity data, comprising:

receiving a present user video image corresponding to user identity data;

communicating the authorized user video image to a remote video image receiver;

storing the authorized user video image at the remote video image receiver;

determining image difference information between the present user video image and the authorized user video image;

transmitting the difference information to the remote video image receiver;

combining the authorized user video image and the difference information to form an output user video image at the remote video image receiver; and

displaying the output user video image.

17. The coding method of claim 16, wherein the present user video image and the authorized user video image are each framed to include only the head and face portions of the user.

18. The coding method of claim 17, wherein the image difference information is determined only for selected portions of the authorized and present user video images.

19. The coding method of claim 18, wherein the selected portions include a mouth region and an eyes region of the authorized and present user video images.

20. The coding method of claim 16, wherein the authorized identity data and the user identity data are MPEG4 objects.